SECRET

CIA INTERNAL
USE ONLY

5 August 1970

MEMORANDUM FOR: CIA COINS Subsystem Manager
CIA Member, Intelligence Information Handling Committee
Chairman, Information Processing Board

SUBJECT : COINS Computer System Planning

1. This memorandum is concerned with the means for providing all-day Headquarters participation in COINS. At the outset, it should be emphasized that a change in the Headquarters computer set-up for COINS is highly desirable even without the all-day requirement. The cost of our current schedule of devoting three hours on the IBM 360/67 each working day to COINS is about $26,000 per month. More important is the loss of the computer during these hours to those in the Agency who have come to depend on it for on-line program development, file handling, and computational support.

2. I believe that the Agency should acquire a computer for Headquarters participation in COINS; that this computer should be dedicated to COINS and to other applications requiring external access; and that CRS should be given the responsibility for operating it. What follows is an attempt to justify this recommendation. The discussion is limited to fundamental assumptions and options; there is no COINS history nor is there an analysis of all the alternatives. Even with these simplifications, the problem remains a difficult one to reduce to manageable terms.

3. There are two fundamental assumptions on which this memorandum is based. If either is wrong, the remaining points are invalid:

CIA INTERNAL
USE ONLY

SECRET

SUBJECT: COINS Computer System Planning

a. It is assumed that the Director of Security will continue to have sufficient doubts regarding computer security so as to advise the Director against storing Agency-sensitive data on a computer which has some possible data path to an uncontrolled terminal. By "some possible data path" is meant a path through computer and communication devices whose internal connections or logical abilities to inhibit the path cannot be guaranteed to function properly. By "uncontrolled terminal" is meant a terminal in an area and accessible to people outside direct Agency control, such as those in the COINS network.

b. It is assumed that the concept of direct remote access by a person in one intelligence agency to computer files stored in another is valid and that economical and technical solutions and reinforcement of need will occur in the next few years.

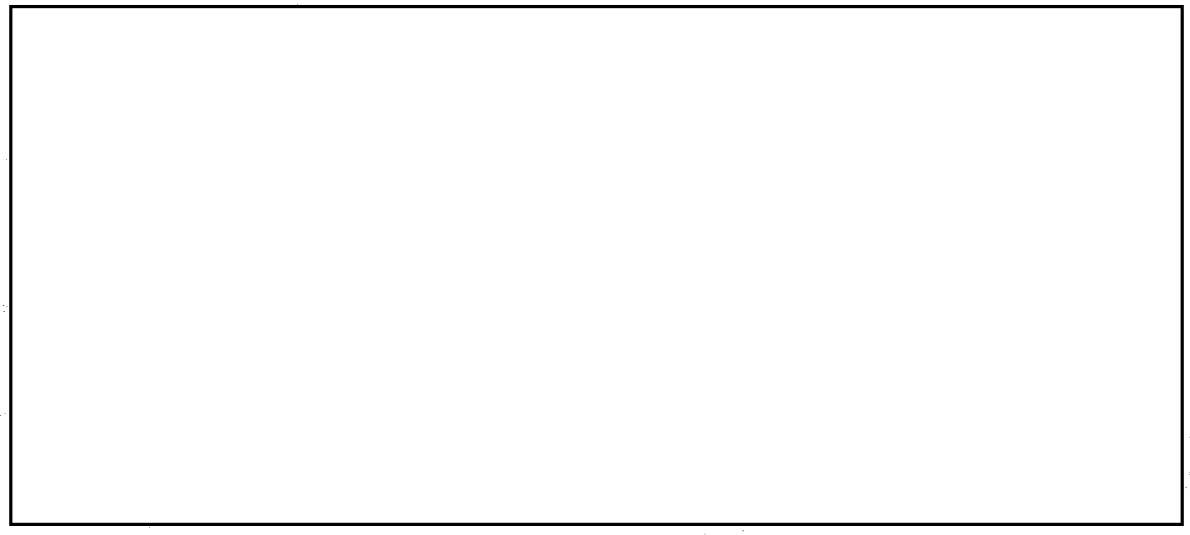
4. Some personal comments on these assumptions. Several safeguards are now employed and additional ones have been suggested to avoid an unwanted path between Agency-sensitive data and uncontrolled terminals: security features in computer software and hardware, data encoding, and communication line monitoring, among others. I believe that these safeguards, alone or in combination, fall short of being both totally effective and operationally feasible. Secondly, I believe the Agency can and should lead the way to an effective community system for computer file access. The question of which should come first - the need or the system - is not raised here.

5. Given the first assumption mentioned above, one must conclude that the Agency's computer facilities must be augmented if we are to operate COINS all day and still meet all our internal needs. This is so because the physical separation of Agency-sensitive data from uncontrolled terminals requires the establishment of at least two physically distinct systems (a "system" might have more than one computer). Only one of these systems would have uncontrolled terminals attached to it (for COINS). The other system could then

SUBJECT: COINS Computer System Planning

safely handle applications involving Agency-sensitive data. Note that physical separation implies that the two systems could not share file storage; if users on one system required access to data stored on the other system, it would have to be duplicated. Further, the equipment on one system could not be used as emergency backup for the other. We achieve the equivalent of physical separation today by scheduling; that is, by defining an OCS computer as the COINS system exclusively at certain times.

6. If the need for two distinct physical systems is accepted, we must decide on which of the two systems we should put the large group of applications left out of the discussion thus far: those internal applications not involving Agency-sensitive data. Two introductory comments relevant to this discussion: 25X1



The size and characteristics of COINS-like applications and Agency-sensitive applications have an effect on the question of where to put the remaining non-sensitive, internal applications. Here we have three choices:

a. Distribute the non-sensitive, internal applications between the two systems. That is, put some on the same

7. Because I prefer the dedicated COINS computer option, the difficulty just noted should be addressed. The second assumption, the validity of community access to computer files, comes into play here. If accepted, this assumption forces us to acknowledge that the cost of the COINS computer must be accepted not just as a price for "going along" with a community file concept, but as the price for self-imposed security constraints. In other words we should not only ask is COINS worth it, but also ask is the protection of SANCA (et al) data worth it? To the latter question, it seems we should say yes. This question should not be shifted to the hopeful "can't the technicians find a way to . . . . ?" In short, the security costs are present in all the options open to us; in the COINS computer option, they are just more visible.

8. Final question: What should be the COINS computer and who should operate it? I believe the organization given responsibility to operate this computer should have the authority to select it and develop the necessary software. I recommend that CRS do this; the COINS objectives, at least as defined by CIA, are within the CRS mission. Although CIRIS and perhaps other follow-on requirements for external access do not fit this argument, I believe these applications should also be handled on the COINS computer for the reasons noted above. In any case, I would expect COINS to dominate this group of applications. CRS should be given the funds and any logistical and technical help they feel they need to develop a COINS system. CRS would continue to be responsible for the COINS data base. OCS would provide them with a copy of that portion of the CIRIS data base which is authorized for outside access. A stand-alone computer to handle COINS and CIRIS would cost between $21,000 and $36,000 per month, depending on the configuration chosen and on software, reliability, compatability factors. Three potential systems are detailed in Attachment 2.

9. A list of several other alternatives which have been considered (and reconsidered) for all-day COINS service at Headquarters is given in Attachment 3. For convenience, they are grouped and discussed in five general categories. The comments are

subjective and are tied to the assumptions and arguments in this memorandum. Additional information on these alternatives and their many variants is available in OCS.

10. Again, I would like to emphasize that even without external prodding, a change in current COINS procedures in Headquarters is highly desirable.

25X1

[redacted]

Acting Director of Computer Services

Attachments: a/s

cc: D/CRS

25X1 [redacted]

OCS Rem & Staff Chiefs